

## ABSTRACT OF THE DISCLOSURE

Cookie files received from cookie file sources (e.g., Internet websites) are screened based upon the recommendations of a service provider which downloads privacy protection criteria in the form of a "watch list" to a subscriber's client machine. A user-friendly interface

5 allows the subscriber to optionally modify the watch list prior to it being used at the subscriber's client machine by assigning known cookie file sources to either a "trustlist" or a "blacklist." A "composite list" is then generated and used by the client machine to screen cookie files. The subscriber receives updates from the service provider on either a periodic or "as-needed" basis using a "quick update algorithm." A "privacy scanning algorithm" runs on the client machine

10 and has two different modes of operation. The first is a continuous mode where unwanted cookie files are blocked from being stored at the client machine. The second is a periodic mode where the client machine is "scrubbed" of unwanted cookie files according to the privacy protection criteria.

TOP SECRET 4302850